Abstract

A message to be transmitted through a network is encrypted such that the resulting encrypted message has associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities. Each of at least a subset of the servers of the network includes a module for checking the proof of correctness if the corresponding encrypted message passes through the corresponding server in being transmitted from a sender to a recipient through the network. The encrypted message is therefore transmitted through the network to the recipient such that in traversing the network the proof of correctness associated with the encrypted message is checked by a designated check module of at least one server of the network. If the check of the proof of correctness indicates that the proof is invalid, the module of the server performing the check may direct that the encrypted message be discarded.